广州市品高软件开发有限公司 ISMS 审核案例

认证机构：广州赛宝认证中心

审核类型：信息安全初次审核

审核员：肖锟（组长）；

1、 案例发生的背景

受审核方广州市品高软件开发有限公司注重人力资源建设、坚持技术创新和管理创新，不断更新软、硬件设备和信息化支持工具，具备了整套自主开发、研究创新和分析能力。为确保生产工作的顺利进行，2014 年该公司依据 GBMS/T 22080-2008/ISO/IEVSN 27001：2005 标准建立了信息安全管理体系。

2014 年是对广州市品高软件开发有限公司的初次审核，如何结合审核给公司提供一些有价值的审核成为本次审核的关注要点。

2、 审核案例发现和沟通过程

企业维持正常业务运转需要依靠硬件、软件、人员、信息等各类资产，如果其中一项或多项资产由于某种原因无法使用，公司的正常业务就会受到影响。这些资产缺失的时间越长，公司恢复正常运作就需要花费越长的时间。为防止公司业务活动中断，

保护关键业务过程免受信息系统重大失误或灾难影响，并确保及时恢复，在国标 GB/T 22080-2008/ ISO/IEC 27001:2005 A.14.1.3 明确提出企业在业务连续性管理的信息安全方面应制定和实施包含信息安全的连续性计划。

在审核支撑广州市品高软件开发有限公司日常业务运作的应用系统时发现该应用系统存在中断或失败后不能在业务需要的水平和时间内恢复的风险。

广州市品高软件开发有限公司依据标准制定了《业务持续性计划和管理程序》，依据该程序文件对各支撑业务的各信息系统进行管理。公司在 3 台 DC 上运行应用系统，每台 DC 都拥有独立的 GC 及数据库，单台机器可以独立工作，就算其中有一台损坏在 DC 网络可通的情况下可以自行切换到另外一台正常的 DC 进行工作，各 DC 间进行数据同步。

但我们在审核时，发现：

（1） 通过查看公司提供的《业务持续性和影响分析报告》，知道广州市品高软件开发有限公司最重要的信息系统是运行在 DC 上的应用系统，该应用系统统管生产和管理调度，具有高度保密性、可用性和完整性。

（2） 访谈业务人员了解到员工需要通过网络才能访问 DC 上的应用系统，DC 应用系统的用户访问控制借助 AD 域实现。公司在 AD 域上采用单域环境，总共分布在 2 个地方，有 3

台域控制器。AD 域用于公司人员账号管理、文件及应用系统的权限认证、普通 PC 机的管理及控制。

（3） 访谈相关人员，相关人员认为维护 DC 应用系统涉及的人员不多，口头交流讨论即可确定连续性方案，未制订书面的应用系统相关的连续性实施计划，且口头商定的连续性方案仅涉及 DC 应用系统本身，未涉及网络和 AD 域的恢复。查现场提供了《业务持续性管理计划测试报告（DC 应用系统）》和《业务持续性管理计划评审报告（DC 应用系统）》。

问题分析：

（1）尽管公司口头讨论了连续性方案并实施，但在实际灾难来临时，许多操作人员常常惊慌失措而遗漏相关步骤。此外，非书面文档也会使得相关参与人员难以测试和修订连续性方案，并难以持续改进。

（2）由于 DC 应用系统的运行需要网络和 AD 域的支持，如果网络或 AD 域不能正常工作的话，则员工无法使用 DC 应用系统，公司业务也难以正常开展。因而公司在考虑 DC 应用系统的业务持续性时还需要考虑网络、AD 域的备份和恢复事宜。

（3）对灾难应对的大部分工作主要由系统部网络管理员负责，公司也规定了网络管理员不在现场时由系统部负责人承担网络管理员的职责，但在访谈时发现部门负责人并不知晓关键主机的具体 IP 地址，对于备份数据所处位置和防火墙策略设置的具

体细节也不太清楚。**存在着灾难来临需要恢复系统和防火墙策略而网络管理员不在公司现场时，系统部负责人无法及时找到所需数据，应用系统不能及时恢复使用的重大风险。**

依据以上审核发现和问题分析，审核组开具了不符合项：**“现场提供的《业务持续性管理实施计划（应用系统）》未描述具体的实施方案。”**

3、 改进及取得的成效

经以上分析，广州市品高软件开发有限公司领导对我们发现的问题欣然接受，并表示此次审核员指出的都是系统安全存在隐患的薄弱环节，需要通过技术、行政等手段加强整改。DC 应用系统是广州市品高软件开发有限公司的核心系统，一旦该系统不能及时恢复，就会造成关键竞争力的削弱、业务的中断，也会给合作伙伴和客户的信心造成沉重打击，因此应从细微之处着眼，未雨绸缪。现场审核后，广州市品高软件开发有限公司对提出的不符合项进行原因了分析并采取了纠正和纠正措施。同时，举一反三，排查同类问题一并整改，取得了良好的管理成效。

改进过程：

（1） 编制具体的《业务持续性管理实施计划（DC 应用系统）》，识别 DC 应用系统可能有的 DC 网络不通、DC 应用系统数据库不同步、DC 硬件故障、DC 应用系统数据损坏、AD 用

户被误删除等风险。并据此给出相应的解决办法。

（2） 认识到 DC 应用系统的正常运行还需要其它设备和资源的配合。为此，对与 DC 应用系统业务持续性管理实施计划相关的技术操作细节，如备份与恢复、网络故障、防火墙策略等形成《windows server 2008 备份与恢复》、《网络故障排查手册》、《防火墙策略》之类的作业文档。

（3） 修订《业务持续性计划和管理程序》，明确要求持续性计划应包括预防、防护、紧急响应、业务恢复等多方面的活动，这些活动必须制定为具体的可实施方案。

取得的成效：

（1） 提高了人员对安全操作文档化的意识。现今公司人员普遍工作繁忙，认为业务连续性操作的诸多事宜口头讨论确定就可以了，没有意识到突发事件对人们处理问题的压力。同时，通过连续性方案的文档化，也能够更好的让相关人员知道如何执行和模拟演练，并发现原有连续性方案的不足，以更好的更新和改进。

（2） 提高了员工对信息安全业务持续性的系统认识。公司识别出了 DC 应用系统是支撑业务的关键系统，但并未意识到员工使用 DC 应用系统还需要网络和 AD 域控的支持。简单的考虑 DC 应用系统的恢复是不够的，灾难来临的形式是多样的，可能会是网络中断、也可能会是域控失败，这些都会导致 DC 应用系

统不可用。因此，在制订业务连续性方案时，不应只孤立的考虑应用系统本身不可用的情况，还需要考虑到其它会造成应用系统不可使用的情况。整体和系统的考虑才能较好的确保 DC 应用系统的恢复能力。

（3） 业务连续性计划成为了企业管理的一部分。由于新修订的《业务持续性计划和管理程序》明确持续性计划包括的活动和必须制定的可实施方案。业务连续性计划已经成了公司日常工作的一部分，确保了该计划的切实可行。

（4） 企业反映此项改进为其更具操作性的实施应急演练找到了更好的方法，通过制订与业务连续性相关的一系列计划和文档，不但确保了演练的持续改进，而且在模拟演练中也证明在网络管理员不在现场的情况下，其他人员也能依据计划和相关文档及时恢复应用系统，有效的减轻了只能依赖网络管理员恢复应用系统的重大风险。审核组将会在今年的监督审核中对这个不符合项的改进作现场验证。

4、 总结

过去，人们有一种误解认为兵来将挡、水来土掩，听天由命，灾难是没法应对的。没有意识到在突发事件来临前就应做出应对计划和方案，以将灾难的损失降到最低，尽快的恢复公司业务。公司管理层应审时度势、未雨绸缪，统筹考虑成本和收益之间的平衡，建立风险可控的、系统化的信息系统恢复方案，确保业务

的及时恢复。业务连续性是一种预防性机制，它明确公司的关键业务以及对业务可能造成的威胁，并据此采取相应的技术手段，制定计划和流程，确保这些关键职能在任何环境下都能持续发挥作用。体系化的业务连续性方案有如下作用：

（1）为公司的日常生产和管理等提供了一套系统、有效的信息安全保障机制，避免因各种信息安全突发事件影响公司业务。

（2）有效保护公司的各种信息数据，增强公司在市场上的竞争力，提高公司的社会效益。

（3）将业务连续性方案融入到企业的日常运作中，减少关键信息系统中断对业务造成的影响，保持公司的市场竞争力。